PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-081519
(43)Date of publication of application : 28.03.1997

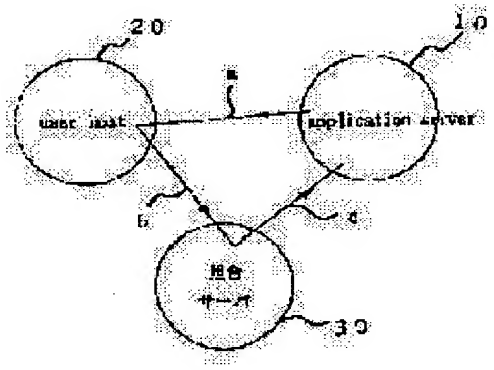
(51)Int.Cl. G06F 15/00

(21)Application number : 07-231160
(22)Date of filing : 08.09.1995

(71)Applicant : KIYADEITSUKUSU:KK
(72)Inventor : TABUKI TAKAAKI

(54) AUTHENTICATION METHOD ON NETWORK

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method which easily authenticates a user on a network.
SOLUTION: An application server 10 requests a user host 20 to send authentication data to a collation server 30. The collation server 30 preliminarily holds correct authentication data in a data base and compares and collates authentication data sent from the user host 20 with correct authentication data. The collation result is sent to the application server 10. The application server 10 authenticates the user based on the result. As a result, the constitution of the application server is simplified. The collation server 30 can be used by plural application servers 10 to efficiently operate the resources on the network.



LEGAL STATUS

[Date of request for examination]	03.06.1997
[Date of sending the examiner's decision of rejection]	06.07.1999
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	11-12880
[Date of requesting appeal against examiner's decision of rejection]	05.08.1999
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－81519

(43)公開日　平成９年(1997)３月28日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　15/00	３３０		Ｇ０６Ｆ　15/00	３３０Ｂ	

審査請求　未請求　請求項の数２　ＯＬ　（全９頁）

(21)出願番号　特願平7－231160

(22)出願日　平成７年(1995)９月８日

(71)出願人　591210910
株式会社キャディックス
東京都世田谷区新町２丁目26番15号

(72)発明者　田吹　隆明
東京都世田谷区新町２丁目26番15号　株式会社キャディックス内

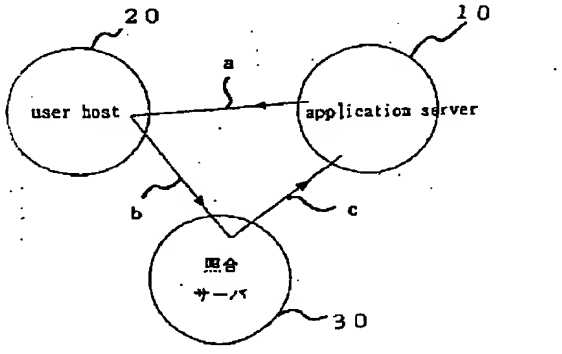
(74)代理人　弁理士　吉田　研二　（外２名）

(54)【発明の名称】　ネットワーク上の認証方法

(57)【要約】

【課題】　ネットワーク上で利用者の認証を容易に行う方法を実現する。

【解決手段】　ユーザホスト２０に対し、アプリケーションサーバ１０は、認証データを照合サーバ３０に送出するよう要求する。照合サーバ３０は、「正しい」認証データを予めデータベースに保持しており、ユーザホスト２０から送出されてきた認証データと、「正しい」認証データとを比較照合する。そして、この照合の結果がアプリケーションサーバ１０に送出される。アプリケーションサーバ１０はこの結果に基づき、利用者に認証を与える。この結果、アプリケーションサーバ１０の構成が簡易化される。照合サーバ３０は、複数のアプリケーションサーバ１０から利用することができ、ネットワーク上の資源の運用の効率化を図ることができる。



1

【特許請求の範囲】
【請求項１】　ネットワーク上のアプリケーションサーバが、そのアプリケーションの利用者の認証を行う認証方法において、
前記アプリケーションサーバが、前記利用者に対し、認証データを照合サーバに送信するよう要求する認証データ要求工程と、
前記利用者が、前記認証データ要求工程におけるアプリケーションサーバの要求に対して、前記利用者の認証データを、前記利用者の識別データと共に、照合サーバに送出する送出工程と、
前記照合サーバが、前記送出されてきた認証データが、前記送出されてきた識別データの利用者の認証データであるか否かを照合する照合工程と、
前記照合サーバが、照合結果を前記アプリケーションサーバに返送する照合結果返送工程と、
前記照合結果返送工程において返送された照合結果に基づいて、前記アプリケーションサーバが前記利用者が正当な利用者であるか否かを認証する認証工程と、
を含むことを特徴とするネットワーク上の認証方法。
【請求項２】　ネットワーク上のアプリケーションサーバが、そのアプリケーションの利用者の認証を行う認証方法において、
前記アプリケーションサーバが、前記利用者に対し、認証データを照合サーバに送信するよう要求する認証データ要求工程と、
前記アプリケーションサーバが、照合サーバに対し、前記利用者の識別データを送信して、前記利用者の正しい認証データを予め呼び出しておくよう要求する照合準備要求工程と、
前記利用者が、前記認証データ要求工程におけるアプリケーションサーバの要求に対して、前記利用者の認証データを、前記利用者の識別データと共に、照合サーバに送出する送出工程と、
前記照合サーバが、前記送出されてきた認証データが、前記送出されてきた識別データの利用者の認証データであるか否かを照合する照合工程と、
前記照合サーバが、照合結果を前記アプリケーションサーバに返送する照合結果返送工程と、
前記照合結果返送工程において返送された照合結果に基づいて、前記アプリケーションサーバが前記利用者が正当な利用者であるか否かを認証する認証工程と、
を含むことを特徴とするネットワーク上の認証方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、アプリケーション利用者の認証を行う方法に関する。特に、ネットワーク上における利用者の認証に関する。
【０００２】
【従来の技術】銀行などのサービス業では、取引に際して、相手が本人であるか否かを確認すること、すなわち認証は極めて重要な問題である。これは、他人が本人になりすまして口座からお金を引き出してしまったり、お金を振り込んでしまったりすることを防止するためである。

2

【０００３】この認証のためには、古典的には例えば、運転免許証や、一定の身分証明書等を提出してもらい、本人であるか否かを確認している。近年、現金自動引き出し器等の発達により、磁気カードやパスワードなどによって、本人の認証を行う方法が広く採用されている。
【０００４】このような「認証」は、銀行以外でも必要とされる場合は多い。例えば、研究機関などにおいては、秘密漏洩を防止すべく、一定の区域へは許可された者のみ入場を許し、それ以外の者に対しては入場を制限する場合が多い。また、会員制クラブ等でも会員であることを何らかの方法で確認しなければならない。この研究機関や会員制クラブにおいても、上記磁気カードやパスワード、若しくは会員証等を用いることも好適である。しかし、磁気カードや会員証は紛失してしまう可能性があるし、また、パスワードも忘れてしまう可能性も決して小さくはない。そのため、本人を確認する方法として、指紋や、網膜パターン等のいわゆるバイオメトリックな物理量を認証のためのデータ（以下、認証データという）として用いる方法も提案されている。
【０００５】企業内の電子ドキュメント承認プロセスでは、署名を用いて本人であることを確認し、承認することが自然である。また近年、企業ではＣＡＤの利用が一般化しており、その承認のプロセスでは署名データの形状をイメージデータとしてＣＡＤデータにはりつけることもできる。
【０００６】
【発明が解決しようとする課題】近年、ネットワークの発達により、このネットワーク上で種々のサービスの提供が行われるようになった。例えば、いわゆるインターネットにおいては、WWW（World Wide Web）等によるマルチメディアタイトルの提供サービスが広く行われている。このようなサービスの提供においては、一般の銀行等におけるサービスと同様に、一定の資格者にのみアクセスを認める場合もある。このようなネットワーク上のサービスにおいても、従来のサービスと同様に、「認証」はきわめて重要な問題である。
【０００７】しかしながら、ネットワーク上で本人であるか否かの認証をする場合に、上述したバイオメトリックな認証データを用いることは一般にきわめて困難である。例えば網膜パターンや指紋、あるいは掌紋等を入力する装置を各端末に備える必要があり、また、このような物理量をネットワークを介して伝送するための仕組みも新たに必要となってしまう。
【０００８】そのため、ネットワーク上で用いられるバイオメトリックな物理量として、署名データを用いるこ

とが注目されている。この署名データは、いわゆるタブレットにより容易に入力することができ、かつ平面の２次元データだけではなく、署名を書くスピードや筆圧の変化もデータとしているため、本人であるか否かを確認するための認証データとして優れた特性を有している。更に、タブレットは一般に安価に構成できるので、端末のコストも安く抑えることができるという特徴を有している。

【０００９】以上述べたように、パスワードなどの認証データの他、署名データ等のバイオメトリックな認証データがネットワーク上における「認証」に利用されている。

【００１０】ところが、ネットワークの拡大にともない、サービスの提供者であるアプリケーションサーバの種類が増え、かつそのサービスの提供を受けるクライアントの数もきわめて膨大なものとなっている。そのため、各アプリケーションサーバがそれぞれ別個に認証を行う際の負担が過大になってきている。特に、インターネットのように世界規模で拡がっている場合には、アプリケーションサーバとそのサービスの提供を受けるクライアントとの間がきわめて遠距離となる場合も多い。このような場合に、認証データのやりとりをすることがネットワーク上のトラフィックの増大に結びついてしまうことも考えられる。

【００１１】本発明は、このような課題を解決するためになされたものであり、その目的は、ネットワーク上のクライアントの認証のための照合の機能をアプリケーションサーバと独立してネットワーク上に設けることによって、アプリケーションサーバの負荷を減少させるとともに、クライアントの認証を容易に行うことが可能な認証方法を提供することである。

【００１２】

【課題を解決するための手段】第１の本発明は、上記課題を解決するために、ネットワーク上のアプリケーションサーバが、そのアプリケーションの利用者の認証を行う認証方法において、前記アプリケーションサーバが、前記利用者に対し、認証データを照合サーバに送信するよう要求する認証データ要求工程と、前記利用者が、前記認証データ要求工程におけるアプリケーションサーバの要求に対して、前記利用者の認証データを、前記利用者の識別データと共に、照合サーバに送出する送出工程と、をまず含んでいる。

【００１３】このように、本発明は、アプリケーションサーバが認証データを外部の照合サーバに送出し、照合の手続きを外部に委託している点に特徴がある。外部に照合の手続きを委託することにより、アプリケーションサーバ自体は照合のためのデータベースを備える必要がなくなる。

【００１４】そして、第１の発明は、前記照合サーバが、前記送出されてきた認証データが、前記送出されてきた識別データの利用者の認証データであるか否かを照合する照合工程と、前記照合サーバが、照合結果を前記アプリケーションサーバに返送する照合結果返送工程と、前記照合結果返送工程において返送された照合結果に基づいて、前記アプリケーションサーバが前記利用者が正当な利用者であるか否かを認証する認証工程と、を含むことを特徴とするネットワーク上の認証方法である。

【００１５】このような構成によって、本発明によれば、アプリケーションサーバ自体が認証データを保持する必要がなく、且つ、認証に必要な「照合」という手続きを照合サーバに集中して担わせることが可能である。

【００１６】次に、第２の本発明は、ネットワーク上のアプリケーションサーバが、そのアプリケーションの利用者の認証を行う認証方法において、前記アプリケーションサーバが、前記利用者に対し、認証データを照合サーバに送信するよう要求する認証データ要求工程と、前記アプリケーションサーバが、照合サーバに対し、前記利用者の識別データを送信して、前記利用者の正しい認証データを予め呼び出しておくよう要求する照合準備要求工程、をまず備えている。

【００１７】すなわち、照合すべき認証データがまだ得られていない時点において、あらかじめ利用者が誰であるのかを照合サーバに伝えることにより、照合サーバは「正しい」認証データを予め記憶手段から読み出しておくことができるのである。これによって、照合対象である認証データが、その照合サーバに送られてきた時に迅速に、「照合」動作を行うことができる。

【００１８】そのため、第２の本発明は、上に述べた工程の他は、第１の本発明と同様の以下の工程を含むものである。

【００１９】すなわち、第２の本発明は、上記工程に加えて、前記利用者が、前記認証データ要求工程におけるアプリケーションサーバの要求に対して、前記利用者の認証データを、前記利用者の識別データと共に、照合サーバに送出する送出工程と、前記照合サーバが、前記送出されてきた認証データが、前記送出されてきた識別データの利用者の認証データであるか否かを照合する照合工程と、前記照合サーバが、照合結果を前記アプリケーションサーバに返送する照合結果返送工程と、前記照合結果返送工程において返送された照合結果に基づいて、前記アプリケーションサーバが前記利用者が正当な利用者であるか否かを認証する認証工程と、を含むことを特徴とするネットワーク上の認証方法である。

【００２０】このような構成によって、第２の本発明は、迅速な認証が行える認証方法である。

【００２１】

【発明の実施の形態】以下、本発明の好適な実施の形態を、図面に基づいて説明する。

【００２２】図１には、本実施の形態において、ネット

ワーク上に設けられているアプリケーションサーバ（Ａｐｐｌｉｃａｔｉｏｎ　Ｓｅｒｖｅｒ）１０のサービスを利用するユーザホスト（Ｕｓｅｒ　Ｈｏｓｔ）２０と、ユーザホスト２０の認証の際に利用される照合サーバ（Ｖｅｒｉｆｉｃａｔｉｏｎ　Ｓｅｒｖｅｒ）３０とがネットワーク上に配置されている様子が示されている。

【００２３】本実施の形態において特徴的なことは、ユーザホスト２０の認証の際の照合動作が、アプリケーションサーバ１０において行われるのではなく、アプリケーションサーバ１０とは別体にネットワーク上に設けられている照合サーバ３０を用いて行われていることである。このように、照合動作を行う照合サーバ３０をアプリケーションサーバ１０と独立にネットワーク上に設けることにより、個々のアプリケーションサーバ１０はユーザホスト２０の認証のための「正しい」認証データを保持したり、照合のための機能を有する必要がなくなる。また、図１においてはアプリケーションサーバ１０としてひとつの構成しか示されていないが、ネットワーク上に複数のアプリケーションサーバ１０を設けることも好適であり、この場合にはその複数のアプリケーションサーバ１０から１個の照合サーバ３０を利用して「照合」動作を委託することができ、複数のアプリケーションサーバ１０において従来重複して備えられていた認証データの照合機能を一つにまとめることができ、効率的な資源の運用が可能となる。

【００２４】また、この照合サーバ３０は、ネットワーク上に複数個設けることも好適である。そして、各アプリケーションサーバ１０は、認証の内容に応じて、好適な照合サーバを利用することが可能となる。例えば、認証データとして署名データが用いられる場合と、認証データとして指紋データが用いられる場合とにおいて利用する照合サーバ３０を変えることも考えられる。もしくは、各利用者が自分の認証データを保持している照合サーバ３０を自ら指定することも考えられよう。

【００２５】図１に示されているように、照合サーバ３０をアプリケーションサーバ１０と独立にネットワーク上に設けることにより、認証の際のメッセージのやりとりは例えば図１において矢印で示されるようになる。図１に示されているように、まず、アプリケーションサーバ１０がユーザホスト２０に対して、認証データを照合サーバ３０に送るように要求する（図１においてａで示される）。この認証データは、古典的にはパスワードや会員番号を利用することもできるが、バイオメトリックな物理量、例えば署名データ等を用いることが好適である。特に、上述したように、署名データは、ユーザホスト２０に安価なタブレットを準備するだけで容易に入力することが可能である。

【００２６】ユーザホスト２０は、ａの要求に対して利用者の署名データをタブレットから入力し、利用者の識別データ（例えば会員番号や利用者名）と共に照合サーバ３０にこの署名データを送出する（図１においてｂで示される）。アプリケーションサーバ１０は、ユーザホスト２０が正しい利用者であるか否かを判断するわけであるが、その認証の際に必要な「照合」作用を外部の照合サーバ３０にいわば委託しているのである。このため、照合サーバ３０は、ユーザホスト２０から送出されてきた認証データと識別データを予め記憶しておいて「正当な」認証データと照合する。具体的には、照合サーバ３０はユーザホスト２０が本人であると主張する利用者名と、その利用者の正しい認証データとをデータベースとして内部に保持している。そして、このデータベースを検索することにより、ユーザホスト２０が本人であると主張する利用者についての正しい認証データ（本実施の形態においては例えば署名データ）を取り出す。そして、この取り出された認証データとユーザホスト２０から送られてきた認証データとを比較・照合し、その結果をアプリケーションサーバ１０に送出する（図１においてｃで示されている）。アプリケーションサーバ１０は、この照合サーバ３０から返送されてきた照合結果に基づいてユーザホスト２０に対して認証を行うのである。

【００２７】本実施の形態においては、このように照合の動作を行う部分を、アプリケーションサーバ１０と独立にネットワーク上に設けたので、複数のアプリケーションサーバ１０に共通に重複して設けられていた照合機能を節約することができるとともに、認証動作の確実さを担保することが可能である。

【００２８】なお、アプリケーションサーバ１０としては、インターネット上における例えばＷＷＷサーバや、各種のデータベース等、種々のサービスを提供するサーバが考えられる。

【００２９】図２には、図１に示されているユーザホスト２０やアプリケーションサーバ１０及び照合サーバ３０の詳細な構成を表す構成ブロック図が示されている。図２に示されているように、ユーザホスト２０は、パーソナルコンピュータ等の端末から構成されており、インターネットに接続し、ＷＷＷサーバ４２に接続するためのＷＷＷブラウザのひとつであるネットスケープ（Ｎｅｔｓｃａｐｅ）５２を備えている。なお、本実施の形態ではネットスケープ５２が用いられているが、これはモザイク（Ｍｏｓａｉｃ）等、他のＷＷＷブラウザでもかまわない。ユーザホスト２０はこのネットスケープ５２の他に、利用者が署名データを入力するためのタブレット（Ｔａｂｌｅｔ）５４を備えている。また、このタブレット５４を制御し、署名データを取り出すためのタブレットドライバプログラム５６が備えられている。このタブレットドライバプログラム５６は、アプリケーションサーバ１０から認証データを送出するように要求が来た場合に、その要求をネットスケープ５２を介して受け

取り、タブレット５４を駆動して得られた認証データ（署名データ）を、照合サーバ３０に送出する。なお、図１に示されているメッセージのやりとりａ，ｂ，ｃと同一のメッセージのやりとりに対して同一の符号ａ，ｂ，ｃが図２にも付されている。

【００３０】アプリケーションサーバ１０は、Ｕｎｉｘマシン上に構築される場合が多い。このアプリケーションサーバ１０には、図２に示されているようにマルチメディアタイトルを提供するWWWサーバ４２と、利用者の正当性を確認するための署名照合要求プログラム４４とが備えられている。照合サーバ３０は、アプリケーションサーバ１０と同様にＵｎｉｘ等のマシン上に構築されており、正当な利用者とその利用者の認証データとを登録した登録データ６２を有している。そして、上記ユーザホスト２０から送出されてくる利用者名（利用者の識別コード）にもとづいて、ユーザホスト２０から送出されてきた認証データ（本実施の形態においては署名データ）と予め登録されている「正しい」認証データを照合し、照合結果をアプリケーションサーバ１０の署名照合要求プログラム４４に送出するのである。

【００３１】照合サーバ３０の登録データ６２は、本実施の形態においては、リレーショナルデータベース（以下、ＲＤＢという）によって管理されている。この登録データのＲＤＢ内の様子が図３に示されている。図３に示されているように、登録データは各正当な利用者毎に所定のデータを記録した表の形で記録されている。図３に示されているように、まずフラグ（ｆｌａｇ）は、システムの種々の状態を表すためのフラグであり、例えば削除フラグ（その利用者がシステムから削除されたか否かを表す）等として用いられる。また、システムユニークキー（ＳｙｓＵｎｉｑ　Ｋｅｙ）は、各利用者に与えられるシステムキーであり、照合サーバ３０におけるテーブル（図３に示されている）の中で唯一に定められる。また、登録タブレットタイプは、その利用者が利用するタブレットのタイプを表す。また、署名データ（Ｓｉｇｎａｔｕｒｅ　ｄａｔａ）は、タブレット５４上で動く電子ペンの動きを表す時系列データである。この署名データには、二次元的な位置を表す情報だけではなく、筆圧やペンの速度も含まれているため、本人であるか否かの認証を精度よく行うことが可能である。

【００３２】このように、照合サーバ３０内部のＲＤＢには、システムユニークキーと、署名データとが登録されているため、ユーザホスト２０から送出された来た署名データ及び利用者を表すシステムユニークキーを用いて、この送られてきた署名データが正当なものであるか否かを判断することが可能である。この判断の結果の内容については後で説明する。

【００３３】本実施の形態におけるＲＤＢにおいてはシステムユニークキーと署名データの他に、システム要求項目（Ｓｙｓｔｅｍ　ｒｅｑｕｉｒｅｄ　ｉｔｅｍｓ）と呼ばれる登録項目が記憶されている。図３に示されているように、システム要求項目としては、利用者の名前（Ｎａｍｅ）、利用者の誕生日（Ｄａｔｅ　ｏｆ　ｂｉｒｔｈ）及び利用者の電話番号（Ｐｈｏｎｅ#）が登録されている。これらのシステム要求項目は、システムユニークキーの代わりに用いられるものである。すなわち、システムユニークキーは後述するようにアプリケーションサーバ１０と照合サーバ３０とが保持しているキーであり、利用者を識別するためのキーであるが、利用者は自分に与えられたシステムユニークキーを必ずしも覚えているとは限らない。そのため、利用者が登録されている署名データを確認したい場合等において、システムユニークキー以外で利用者を特定できる手段が存在した方が望ましい。このような場合にシステムユニークキー以外でも、利用者の名前や誕生日、そして電話番号等で利用者を識別し得るようにしたのである。

【００３４】更に、本実施の形態においては、図３に示されているように、オプショナルフィールト（Ｏｐｔｉｏｎａｌ　ｆｉｅｌｄｓ）が設けられている。このオプショナルフィールドに登録されているデータはいわゆるシステム監査用のデータであり、照合サーバ３０のシステムの管理者が照合サーバ３０の動作等を管理する際に用いられる管理データである。図３に示されているように、この管理用のデータとしては、データの作成日（Ｃｒｅａｔｉｏｎ　ｄａｔｅ）、データの作成者（Ｃｒｅａｔｉｏｎ　ｈｏｓｔ）、また、最終アクセス日（Ｌａｓｔ　ａｃｃ．ｄａｔｅ）や、最終アクセス者（Ｌａｓｔ　ａｃｃ．　ｂｙ）、その他アクセス回数（ａｃｃｅｓｓ　ｃｏｕｎｔ）や照合が失敗した回数（ｆａｉｌｕｒｅｃｏｕｎｔ）等、種々のデータを保持することが可能である。

【００３５】また、アプリケーションサーバ１０にも照合サーバ内のＲＤＢに対応して、利用者についての情報を登録したＲＤＢが備えられている。このアプリケーションサーバ１０内のＲＤＢに登録されている内容が図４に示されている。図４に示されているように、各種の登録データが個々の利用者毎に登録されている。図４に示されているように、まず、「照合サーバ名」は、その利用者が送ってきた認証データ（署名データ）がどの照合サーバ３０によって照合されるべきか否かを表すものである。図１に示された構成図においては、照合サーバ３０はひとつしか示していなかったが、ネットワーク内に複数の照合サーバ３０が存在することも構成として可能である。例えば、各利用者は、自分が連絡を取りやすい照合サーバ３０を使用したいと思う場合もあるであろうし、またアプリケーションサーバ１０が各利用者毎に照合サーバ３０を管理上の理由により変更したいと考える場合もあるであろう。

【００３６】図４に示されているフラグ（ｆｌａｇ）とシステムユニークキー（Ｓｙｓ　Ｕｎｉｑ　Ｋｅｙ）と

は、図３におけるフラグ及びシステムユニークキーと同一のものである。このシステムユニークキーは、上述したように、照合サーバ３０のＲＤＢの中で唯一に定められているものである。換言すれば、照合サーバ３０が異なる利用者については、同一のシステムユニークキーが割り当てられる可能性も存在する。したがって、利用者の識別は、厳密には、このシステムユニークキーと照合サーバ名とを組み合わせることにより行われることになる。アプリケーションユーザキー（Ａｐｐ．　ｕｓｅｒ　ｋｅｙ）は、そのアプリケーションサーバ１０の提供するサービスを受けられるか否かを表すキーである。場合によっては図４に示されているように追加アプリケーションユーザキー（Ａｄｄｉｔｉｏｎａｌ　ａｐｐ．　ｕｓｅｒ　ｋｅｙ）が設定される場合もある。更に、図４に示されているように作成日（Ｃｒｅａｔｉｏｎ　ｄａｔｅ）や最終アクセス日（Ｌａｓｔ　ａｃｃ．　ｄａｔｅ）、最終アクセス者（Ｌａｓｔ　ａｃｃ．　ｂｙ）、アクセス回数（ａｃｃｅｓｓ　ｃｏｕｎｔ）、照合が失敗した回数（ｆａｉｌｕｒｅ　ｃｏｕｎｔ）等が図３に示されている照合サーバ３０内のＲＤＢに対応して登録されている。また、具体的な項目名は示されていないが、アプリケーションオプショナルフィールド（Ａｐｐｌｉｃａｔｉｏｎ　ｏｐｔｉｏｎａｌｆｉｅｌｄｓ）にアプリケーションが利用する所定の登録データを登録することも好適である。

【００３７】図５には、本実施の形態に係る照合サーバ３０がサポートするプロトコルの説明図が示されている。図５に示されているように、まずプロトコル「キーの登録」においては、アプリケーションサーバ１０が所定の必須項目を含むメッセージを照合サーバ３０に送出する。照合サーバはこれらの必須項目をＲＤＢに登録すると共に、システムユニークキーを生成する。このシステムユニークキーはＲＤＢに登録されると共に、アプリケーションサーバ１０に返送される。このようにして、利用者を識別するシステムユニークキーが照合サーバ３０において生成される。このシステムユニークキーはアプリケーションサーバ１０においてもＲＤＢ内に登録され、照合サーバ３０とアプリケーションサーバ１０との間でシステムユニークキーの共有がなされる。

【００３８】次に、プロトコル「署名データの登録」においては、アプリケーションサーバ１０が、システムユニークキー、３個の署名データ、タブレットタイプ等を、照合サーバ３０に送出し、「正しい」署名データを照合サーバ３０内のＲＤＢに登録させる。ここで、３個の署名データを送出するのは平均的な署名データの値を照合サーバにおいて求めて、平均的な値をＲＤＢ内に登録するためである。登録が正常に完了すれば、戻り値「ｏｋ」をアプリケーションサーバ１０に返送し、既に登録が行われている場合等には「ｅｒｒｏｒ」を戻り値として返送する。また、３個の署名データが互いに著しく異なりすぎている場合には、署名データとしての信頼性が低いため、登録は行わずに「ｕｎｓｔａｂｌｅ」を戻り値として返送する。

【００３９】プロトコル「照合準備」においては、アプリケーションサーバ１０が、システムユニークキーのみを照合サーバ３０に送出し、「正しい」認証データをＲＤＢからキャッシュに呼び出させておく。このように、実際の認証データとの照合プロトコルに先立って、認証データを予め呼び出させておくことにより、後述するように迅速な照合処理が行えるのである。本プロトコルは、処理の迅速化のために行われるのであり、迅速化が必要でない場合には、本プロトコルを省略し、直接、後述する「照合」プロトコルを発行してもよい。尚、「正しい」認証データの呼び出しが正常に完了した場合にはメッセージＩＤがアプリケーションサーバ１０に返送されるが、エラーが生じた場合には「ｅｒｒｏｒ」を戻り値としてアプリケーションサーバ１０に返送する。

【００４０】プロトコル「照合」は、ユーザホスト２０がシステムユニークキー、署名データ、タブレットタイプ、及びメッセージＩＤを照合サーバ３０に送出し、照合動作を行わせるプロトコルである。尚、メッセージＩＤは、先に「照合準備」プロトコルが発行されている場合にその戻り値として返送されたメッセージＩＤが用いられる。尚、後述するように、照合結果はアプリケーションサーバ１０に送出されるが、その際、このメッセージＩＤはどの利用者の認証であるかを識別するタグとして使用される。すなわち、本実施の形態においては、このメッセージＩＤは、認証の識別用の番号であると共に、キャッシュに認証データが既に呼び出されていることをも表すＩＤでもある。この場合メッセージＩＤの最初の作成は照合サーバ３０が行い、照合準備要求に対する応答の時にメッセージに付与されるのである。

【００４１】一方、もし「照合準備」プロトコルが発行されていない場合には、このメッセージＩＤは、単にどの利用者に対する認証であるのかを識別する識別子としての役割しか果たさない。この場合はメッセージＩＤの最初の作成はアプリケーションサーバ２０である。

【００４２】さて、照合サーバ３０は、このメッセージＩＤが自己が付与したものか否かによって、認証データが既にキャッシュに読み出されているか否かを否かを知ることができる。既に「正しい」認証データが呼び出されている場合には、そのデータと、送られてきた認証データとを比較・照合する。「正しい」認証データが呼び出されていない場合には、ＲＤＢから新たに「正しい」認証データが呼び出されて、比較・照合動作が行われる。

【００４３】比較・照合の結果、両者が非常に近く正しい認証データであると判断される場合には、戻り値として「ｙｅｓ」がアプリケーションサーバ１０に送出される。一方、送られてきた認証データが「正しい」認証デ

ータと全く異なったものである場合には戻り値として「ｎｏ」が送出される。比較・照合の結果、正しい認証データであるか否かが不明な場合は、戻り値として「ｍａｙｂｅ」をアプリケーションサーバ１０に送出する。不明な場合の対処は、各アプリケーションサーバ１０ごとに異なるであろうが、例えば、署名を利用者にやり直させる等の処置が執られることになろう。また、比較・照合をする「正しい」認証データが見つからなかった場合等においては、戻り値として「ｅｒｒｏｒ」がアプリケーションサーバ１０に送出される。

【００４４】次に、実際の利用者の認証が行われる様子を図６に基づいて説明する。以下、この利用者のことをアプリケーションクライアントと称する（図６）まず、アプリケーションクライアントは、ユーザホスト２０を介してアプリケーションサーバ１０に対して、接続要求を行う。

【００４５】これに応答してアプリケーションサーバ１０は、アプリケーションクライアントに対して、アプリケーションキーの入力を要求する。これに応答して、ユーザホスト２０の表示装置上にはアプリケーションキーの入力を促すプロンプトが表示される。

【００４６】アプリケーションクライアントがユーザホスト２０において所定のキーを入力すると、そのデータがアプリケーションサーバ１０に送出される。

【００４７】アプリケーションサーバ１０は、このキーデータを受信すると、署名データの照合準備の要求を照合サーバ３０に送出する。この照合準備要求は、上述したように処理の迅速化のために行うものであり、省略することも可能である。

【００４８】照合サーバ３０は照合準備要求を受信すると、上述したように、認証データをＲＤＢから読み出し、キャッシュに記憶させると共にアプリケーションサーバ１０に対してメッセージＩＤ、暗号キーを送出する。暗号キーは通信データの暗号化に用いられるキーであり、暗号化が必要なければ送らなくともよい。

【００４９】上記メッセージＩＤ等を受信したアプリケーションサーバ１０は、アプリケーションクライアントに署名を入力させるため、署名入力要求を出力する。

【００５０】この署名入力要求に応じてユーザホスト２０においては署名入力プログラムが起動する。このプログラムの起動に基づき、アプリケーションクライアントはユーザホスト２０に備えられているタブレット５４を用いて署名を行う。ユーザホスト２０は、タブレット５４から入力された署名データを認証サーバ３０に送出する（照合要求）。この際、図６に示されているように、キーデータや、メッセージＩＤが署名データとともに、照合サーバ３０に送出される。

【００５１】照合サーバ３０は、照合要求に基づき、照合を行い、その結果をアプリケーションサーバ１０に返送する。照合サーバ３０は、照合要求の際に同時に送られてきたメッセージＩＤ等に基づいて、照合結果を送出すべきアプリケーションサーバ１０を特定することができる。

【００５２】アプリケーションサーバ１０は照合結果に基づき、認証を行う。このときの動作は各アプリケーションサーバ１０により異なるが、照合結果がＹＥＳの場合には「認証」を与えることになり、それ以外の場合には「認証」を与えない、若しくは署名をやり直させることになろう。

【００５３】以上述べたように、本実施の形態によれば、認証の際に行われる照合動作を外部の照合サーバに委託したので、アプリケーションサーバの負荷を減らすと共に照合動作の簡明化を図ることができる。

【００５４】

【発明の効果】以上述べたように、第１の本発明よれば、ネットワーク上における利用者の認証をアプリケーションサーバ以外の照合サーバに行わせたので、アプリケーションサーバの構成が簡単になり、また、複数のアプリケーションサーバが同一の照合サーバを利用することで、ネットワーク上の資源をより効率的に利用することができるという効果を奏する。

【００５５】また、第２の本発明によれば、照合に先立って、照合準備要求工程で、認証データを予め呼び出させておいたので、迅速な照合を行うことが可能である。

【図面の簡単な説明】

【図１】　本発明の実施の形態の構成を表す構成図である。

【図２】　本発明の実施の形態の構成の詳細を表す説明図である。

【図３】　照合サーバ内のＲＤＢの構成を表す説明図である。

【図４】　アプリケーションサーバ内のＲＤＢの構成を表す説明図である。

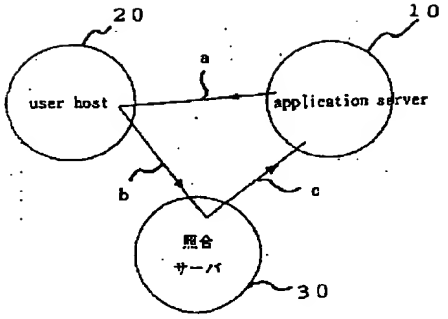
【図５】　照合サーバがサポートするプロトコルを表す説明図である。

【図６】　本実施の形態におけるメッセージの交換を表す説明図である。

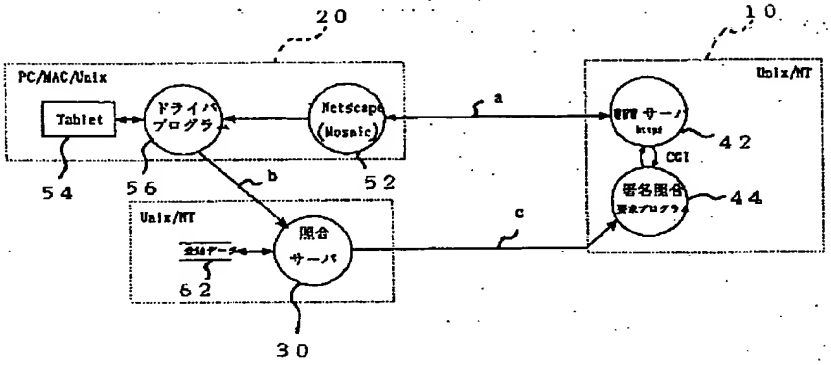
【符号の説明】

１０　アプリケーションサーバ、２０　ユーザホスト、３０　照合サーバ、４２　ＷＷＷサーバ、４４　署名照合要求プログラム、５２　ネットスケープ、５４　タブレット、５６　タブレットドライバプログラム、６２　登録データ。

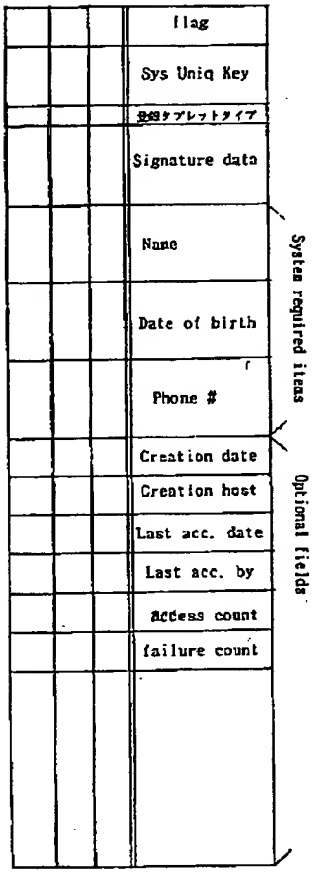
【図1】



【図2】



【図3】



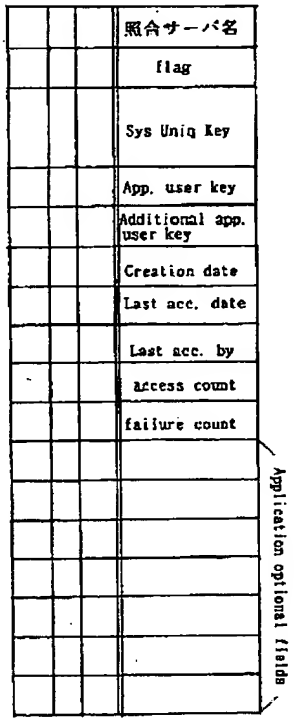
【図5】

照合サーバプロトコル

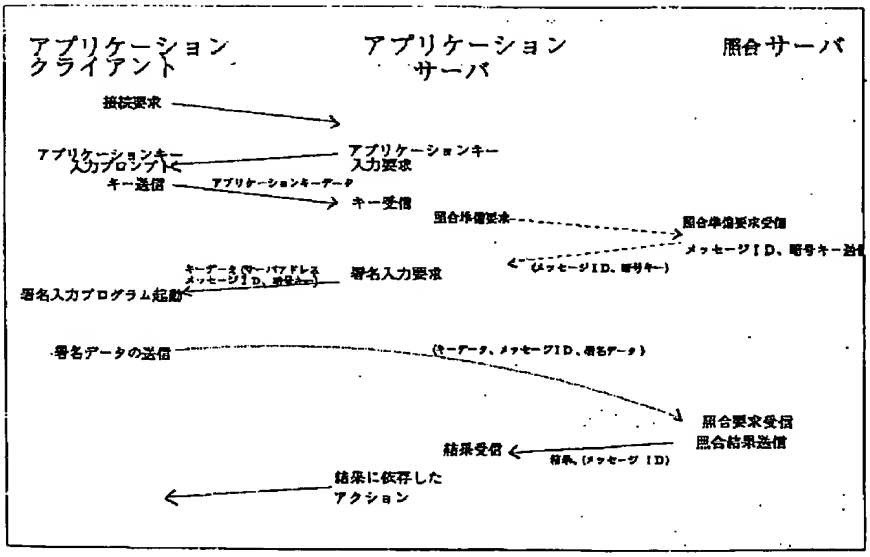
リクエストに共通なデータ：データバージョン、暗号タイプ、圧縮タイプ

リクエスト	リクエストに依存したデータ項目	戻り値	説明
キーの登録	必須項目(Name, BirthDate, Phone)	System uniq key error	照合サーバにシステム必須項目を与えて、 システムユニークキー（登録キー）を得る
署名データの登録	System uniq key, 署名データ xS タブレットタイプ	ok/error: Unstable	登録キーと共に複数の登録用署名データを送信し、 署名の登録をする
照合	System uniq key, 署名データ , タブレットタイプ メッセージID	Yes No Maybe error	登録キーとともに照合される署名をデータを送信して 照合要求をする 照合準備要求をした後であればメッセージＩＤを付ける
照合準備	System uniq key	error メッセージID、暗号キー	照合に先立って登録キーをもとに署名データの読みだし 要求をする。 戻されるメッセージＩＤを使い照合することもできる

【図４】


照合サーバ名
flag
Sys Uniq Key
App. user key
Additional app. user key
Creation date
Last acc. date
Last acc. by
access count
failure count
Application optional fields

【図６】


アプリケーション クライアント
アプリケーション サーバ
照合サーバ
接続要求
アプリケーションキー 入力プロンプト
アプリケーションキー 入力要求
キー送信
アプリケーションキーデータ
キー受信
照合準備要求
照合準備要求受信
メッセージＩＤ、暗号キー送信
(メッセージID、暗号キー)
署名入力要求
署名入力プログラム起動
署名データの送信
(キーデータ、メッセージID、署名データ)
照合要求受信
照合結果送信
結果受信
結果、(メッセージ ID)
結果に依存した アクション